




 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
S1	SR	Security: Access Control	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.	ISO 17799: 9.1.1.2.b; HIPAA: 164.312(a)(1)	N	X		
S2			The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.	Canadian: Alberta 4.1.3 (EMR); CC SFR: FMT_MSA; SP800-53: AC-5 LEAST PRIVILEGE; HIPAA: 164.312(a)(1)	N	X		
S3			The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role-based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)	Canadian: Ontario 5.3.12.e (System Access Management); CC SFR: FDP_ACC, FMT_MSA; ASTM: E1985-98; SP800-53: AC-3 ACCESS AND INFORMATION FLOW CONTROL; HIPAA: 164.312(a)(1)	N	X		
S4			The system shall support revocation of the access privileges of a user without requiring deletion of the user.		N		X	


 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
<b>S5.1</b>	SR	Security: Audit	The system shall be able to generate an audit record when auditable events happen, including but not limited to the following (success, attempt, and failure): User Login/Logout, Chart created/viewed/updated/deleted, and System Security Administration.	CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.312(b)	<b>N</b>	X		
<b>S5.2</b>			The system shall be able to generate an audit record when auditable events happen, including but not limited to the following (success, attempt, and failure): system start/stop, User Login/Logout, Chart created/viewed/updated/deleted, Scheduling, Query, Order, Node-authentication failure, Signature created/validated, PHI export (e.g. print), PHI import, and System Administration.	CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.312(b)	<b>N</b>		X	
<b>S6</b>			The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the information system (e.g., software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.	CC SFR: FAU_GEN; SP800-53: AU-3 CONTENT OF AUDIT RECORDS, AU-10 NON-REPUDIATION; HIPAA: 164.312(b)	<b>N</b>	X		


 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
S7			The system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format and correlate records based on time (e.g., UTC synchronization).	CC SFR: FAU_SAR; SP800-53: AU-7 AUDIT REDUCTION AND REPORT GENERATION; HIPAA: 164.312(b)	Y	X		
S8.1			The system shall be able to provide time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.	CC SFR: FPT_STM; SP800-53: AU-8 TIME STAMPS	Y	X		
S8.2			The system shall record time stamps using UTC based on ISO 8601-2000. Example: "1994-11-05T08:15:30-05:00" corresponds to November 5, 1994, 8:15:30 am, US Eastern Standard Time.	CC SFR: FPT_STM; SP800-53: AU-8 TIME STAMPS	N		X	
S9			The system shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall be able to prevent modifications to the audit records.	CC SFR: FAU_SAR, FAU_STG; SP800-53: AU-9 PROTECTION OF AUDIT INFORMATION; HIPAA: 164.312(a)(1)	N	X		
S10			The system shall continue normal operation even when security audit facility is non-functional. (For example, if the audit log reaches capacity, the system should continue to operate and should either suspend logging, start a new log or begin overwriting the existing log.)	CC SFR: FAU_ARP; SP800-53 AI-5 AUDIT PROCESSING; HIPAA 164.312 (b)	N		X	

 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> © 2006 The Certification Commission for Healthcare Information Technology					<b>Note:</b> Items highlighted in yellow are Provisional for 2006 (see cover letter)			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
S11			The system shall allow an authorized administrator to set the inclusion or exclusion of audited events based on organizational policy & operating requirements/limits.	CC SFR: FAU_SEL; HIPAA 164.312(b)	N			X
S12	SR	Security: Authentication	The system shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed including when not connected to a network e.g. mobile devices.	Canadian: Alberta 1.1; CC SFR: FIA_UAU, FIA_UID; SP800-53: IA-2 USER IDENTIFICATION AND	Y	X		
S13			When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.	Canadian: Alberta 7.3.12 (Security) Canadian Ontario 5.3.12.b (System Access Management); CC SFR: FIA_SOS, FIA_UAU, FIA_UID; ASTM: E1987-98; SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION (no strength of password); ISO 17799: 9.3.1.d; HIPAA: 164.	Y	X		


 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
<b>S14</b>			The system upon detection of inactivity shall prevent further viewing and access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.	Canadian: Alberta 7.3.14 (Security) Canadian Ontario 5.6.12.a (Workstation Security); CC SFR: FTA_SSL, FMT_SAE; SP800-53: AC-11 SESSION LOCK; HIPAA: 164.312(a)(1)	<b>Y</b>	<b>X</b>		
<b>S15</b>			The system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system shall protect against further malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for an [Assignment: organization-defined time period], or delays next login prompt according to [Assignment: organization-defined delay algorithm])	Canadian: Ontario 5.3.12.c (System Access Management); CC SFR: FIA_AFL, FMT_SAE; SP800-53: AC-6 UNSUCCESSFUL LOGIN ATTEMPTS, AC-11 SESSION LOCK ; ISO 17799: 9.3.1.e, 9.5.2.e; HIPAA: 164.312(a)(1)	<b>Y</b>	<b>X</b>		
<b>S16.1</b>			When passwords are used, the system shall provide an administrative function that resets passwords.	CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)	<b>Y</b>	<b>X</b>		


 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
<b>S16.2</b>			When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.	CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)	Y		X	
<b>S17</b>			The system shall provide only limited feedback information to the user during the authentication.	CC SFR: FIA_UAU; SP800-53: IA-6 AUTHENTICATOR FEEDBACK; HIPAA: 164.312(d)	Y	X		
<b>S18</b>			The system shall support case insensitive usernames that contain typeable alpha and numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).	CC SFR: FMT_MTD	Y	X		
<b>S19</b>			When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rule (#13) that allow for minimum number of characters, and inclusion of alpha-numeric complexity.	CC SFR: FMT_MTD	Y	X		
<b>S20</b>			When passwords are used, the system shall support case sensitive passwords that contain typeable alpha and numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).	Canadian: Ontario 5.3.12 (b); SP 800-63	Y	X		
<b>S21</b>			When passwords are used, the system shall not store passwords in plain text.		Y	X		
<b>S22</b>			When passwords are used, the system shall prevent the reuse of passwords within a specific timeframe.	CC SFR: FMT_MTD; ISO 17799 9.5.4.f; HIPAA 164.312(d)	Y		X	
<b>S23</b>			The system shall include documentation that covers: Method used to create, modify, and remove user accounts.	CC SFR: AGD_ADM	Y	X		


 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
<b>S24</b>	SR	Security: Technical Services	The system shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPsec, XML encryptions, or S/MIME or their successors.	Canadian: Alberta 7.4.6.2 & 8.4.6.2 (Technical); CC SFR: FCS_COP; SP800-53: SC-13 CRYPTOGRAPHIC OPERATIONS; HIPAA: 164.312(e)(1)	Y	X		
<b>S25</b>			The system shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPsec, XML digital signature, or S/MIME or their successors.	Canadian: Ontario 5.3.12.a (System Access Management); CC SFR: FCS_CKM; SP800-53: SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT; HIPAA: 164.312(e)(1)	Y	X		
<b>S26</b>			When passwords are used, the system shall not display passwords while being entered.	CC SFR: FPT_ITC; ISO 17799 9.2.3; HIPAA 164.312(a)(1)	Y	X		
<b>S27</b>			If the system provides a web (HTTP) interface, then it shall provide an SSL configuration mechanism. (E.g. This might be a manual that describes the proper configuration steps.)	CC SFR: AGD_ADM	Y	X		

 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
S28			The system shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.	CC SFR: FPT_RCV	Y	X		
S29			The system shall support ensuring the authenticity of remote nodes (mutual node authentication) when communicating Protected Health Information (PHI) over the Internet or other known open networks using open protocol (e.g. TLS, SSL, IPSec, XML sig, S/MIME).	CC SFR: FPT_RCV	Y	X		
R1	SR	Reliability: Backup / Recovery	The system shall generate a backup copy of the application data, security credentials, and log/audit files.	Canadian: Alberta 7.3.16 (Security); CC SFR: FDP_ROL, FPT_RCV; HIPAA: 164.310(d)(1)	Y	X		
R2			The system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.	Canadian: Alberta 7.3.18.9 (Security); CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.310(d)(1)	Y	X		
R3			If the system claims to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.	Canadian: Alberta 7.4.2.5 (Technica+D1I); CC SFR: FDP_ROL; HIPAA: 164.310(d)(1)	Y	X		



 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
R4		Reliability: Documentation	The vendor shall provide documentation on known issues regarding the use of off-the-shelf malware detection and eradication software.	Canadian: Alberta 7.3.17 (Security); CC SFR: FPT_TST; SP800-53: SI-3 MALICIOUS CODE PROTECTION;	N	X		
R5			If the system includes hardware, then the system shall include documentation that covers: Expected physical environment necessary for proper secure & reliable operation of the system including: electrical, HVAC, sterilization, and work area.	CC SFR: AGD_ADM	N	X		
R6			Removed					
R7			The system shall include documentation that covers: The services (e.g. php, web service) and network protocols/ports (e.g. hl7, http, ftp) that are necessary for proper operation and servicing of the system, including justification of the need for that service and protocol. This information may be used by the healthcare facility to properly configure their network defenses (firewalls and routers).	CC SFR: AGD_ADM; SP 800-53 AC-5 CM-6; SP 800-70; HIPAA 164.312(a)(1)	N	X		
R8			The system shall include documentation of known conflicts with security services (e.g. antivirus, intrusion detection, malware eradication, host based firewall, etc.) and the resolution of that conflict.	Canadian: Alberta 7.3.17 (Security); CC SFR: FPT_TST CC SFR: AGD_ADM; SP800-53 SI-3 MALICIOUS CODE PROTECTION	N	X		
R9			The system shall include documentation that covers: The steps needed to confirm that the installation was properly completed and that the system is operational.	CC SFR: AGD_ADM	N	X		

 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> <b>Items highlighted in yellow are</b> <b>Provisional for 2006 (see cover letter)</b>			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
R10			The system shall include documentation that covers: The patch (hot-fix) handling process the vendor will use for EHR, operating system and underlying tools. (e.g. specific web site where patch notices are, approved patch list, special instructions for installation, and post installation test).	CC SFR: AGD_ADM	N	X		
R11			The system shall include documentation that explains system error or performance messages to users and administrators, with actions required.	CC SFR: AGD_ADM	N	X		
R12			The system shall have documentation of product capacities (e.g. number of users, number of transactions per second, number of records, network load, etc.) given a baseline representative configurations (e.g. number or type of processors, server/workstation configuration and network capacity, etc).	CC SFR: AGD_ADM; SP800-53 CM-2	N	X		
R13			The system shall include documented procedures for product installation, start-up and/or connection.	CC SFR: ADO_IGS	N	X		
R14	SR	Reliability: Technical Services	The system, including installation media, shall be free of currently, well-known malware.	CC SFR: ADO_DEL	N	X		
R15			Removed		N			
R16			The system shall include documentation of the minimal privileges necessary for each service and protocol necessary to provide EHR functionality and/or serviceability.	SP800-53 AC-5	N	X		
R17			The system shall be configurable to prevent corruption or loss of data already accepted into the system in the event of a system failure (e.g. integrating with a UPS, etc.).	CC SFR: FPT_RCV	Y	X		

 <b>Final Criteria: SECURITY &amp; RELIABILITY</b> <b>For 2006 Certification of Ambulatory EHRs</b> <b>Effective May 1, 2006</b> <small>© 2006 The Certification Commission for Healthcare Information Technology</small>					<b>Note:</b> Items highlighted in yellow are Provisional for 2006 (see cover letter)			
Line #	WG	Category and Description	Specific Criteria	Source or References	Items Assignable* (see below)	Compliance		
						Certify in May 2006	Roadmap for May 2007	Roadmap for May 2008 and beyond
R18	SR	Reliability: Documentation	The system shall include documentation that covers: Guidelines for proper configuration of the EHR security controls (e.g. users, roles management, password management, audit logs) necessary for proper secure and reliable operation of the system.	CC SFR: AGD_ADM	N		X	
R19			Removed					

**\*Assignable Functions:**

Applicants may assign certain functionality to a third party (e.g. when security and operating functions are handled by the operating system, a third party component, tool or service, etc.). Where a function is indicated as “assignable”, applicants can indicate they are delegating and provide related materials for self attestation. For example – for backup and restore: applicants that use a third party database backup utility could assign backup functionality and provide related documentation for self-attestation.